Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# QUANTUM CRYPTOGRAPHY FOR SECURE CLOUD DATA STORAGE AND TRANSMISSION

**RAHUL SURYODAI [1], DESIDI NARSIMHA REDDY[2], DR. HEMLATA MAKARAND JADHAV [3], ANIL KUMAR MUTHEVI [4], DR. V. V. R. MAHESWARA RAO [5], V SIVARAMARAJU VETUKURI [6]**

[1]Senior Data Engineer (Data Governance, Data Analytics: enterprise performance management, AI&ML),USA.
[2] Data Consultant, Soniks consulting LLC, 101 E park blvd, suite no: 410,Plano,TX, 75074,USA.
[3] Department of E&TC, Marathwada Mitra Mandal's College of Engineering, Pune, India.
[4] Department of Computer Science and Engineering, Aditya University, Surampalem, India.
[5] Shri Vishnu Engineering College for Women, Department of Computer Science and Engineering, Bhimavaram, India.
[6] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India

E-mail: [1]rsuryodai@outlook.com, [2] dn.narsimha@gmail.com, [3] hemakj123@gmail.com, [4] lettertoanil@gmail.com, [5] mahesh_vvr@yahoo.com, [6] sivaramaraju.vetukuri@gmail.com

**ABSTRACT**

Traditional encryption algorithms like RSA and ECC are increasingly vulnerable due to advances in quantum computing, which enable attacks through techniques such as Shor's and Grover's algorithms. To address this challenge, the researchers proposed a hybrid encryption system that integrates Quantum Key Distribution (QKD) with the Advanced Encryption Standard (AES-256) to ensure secure data transmission and storage in cloud environments. The system employs the BB84 protocol over a virtual 50 km quantum channel for key generation and distribution. Additionally, introduce the Hybrid Secure Transmission Protocol (HSTP) that rotates session keys every 5 seconds, enhancing security through continuous key renewal. By adapting the Key Management Service (KMS) to utilise QKD-generated keys, this approach is compatible with popular cloud platforms such as AWS S3 and Google Cloud Storage. Experimental evaluations comparing AES+QKD with conventional AES+RSA demonstrate that AES+QKD achieves higher key generation rates (>1050 MB/s), superior data consistency (99.9%), and maintains low latency under heavy workloads, while effectively resisting both classical and quantum attacks. This work presents a scalable, quantum-safe cloud security architecture, showcasing the practical integration of QKD in large-scale cloud infrastructures through the novel HSTP protocol and validated performance models.

**Keywords:** *Quantum Key Distribution (QKD), AES-256 Encryption, Cloud Data Security, Post-Quantum Cryptography, Hybrid Secure Transmission Protocol (HSTP).*

## 1. INTRODUCTION

Due to the rapid development of quantum computing, algorithms like Shor and Grover might demolish the mathematical foundation of popular cryptographic systems like the RSA and ECC [1]. The need to provide durable data protection within a cloud environment under the condition of quantum computing power has become so urgent due to the emergence of this risk [2]. As cloud storage and transmission cases have sensitive data being transferred and updated, revealing secrets to unknown competitors in the future, confidentiality, integrity, and availability, even with quantum adversaries, should be ensured.

Not all cryptography is vulnerable to the advances of computing power that can crack traditional encryption [3]. Quantum cryptography, especially quantum key distribution (QKD), has an information-theoretic model based upon the laws of physics and is hence secure against any advance in computing power. The research problem that is going to be discussed in the current paper is the possibility of combining QKD with high-performance symmetric encryption, which is AES-256, in order to obtain quantum resistance as well as

practical efficiency in a cloud-based implementation [4].

This paper covers the design and deployment of a hybrid AES+QKD system in popular cloud infrastructure providers like AWS S3 and Google Cloud Storage, and is tested [5]. The most significant ones are the devised hybrid secure transmission protocol (hstp) that can be used to rotate keys without impairing flow, experimental measurement of the observed performance parameters like throughput, latency, and scalability, and an elaborate security analysis on both the classical and quantum attacks [6]. This work bridges the gap between theoretical models of quantum cryptographic algorithms and their application to large-scale, mission-critical cloud environments, demonstrating the practicality and high performance of a quantum-safe solution, further enhanced by the Hybrid Secure Transmission Protocol (HSTP) introduced in this study.[7].

## 2. RELATED WORKS:

In the last four years, work in the realm of secure transmission of data in clouds has developed across three primary directions [8]. Initially, there have been works to improve classical cryptography in the cloud to optimise symmetric encryption (AES-256) and public-key systems (RSA, ECC) using scalable Key Management Services (KMS) and Hardware Security Modules (HSM) in the cloud. Even though these methods are generally compatible with the existing systems, they are susceptible to attacks by a large-scale quantum computer [9]. Second, there have been considerable advances in Quantum Key Distribution (QKD) algorithms, such as the demonstration of BB84, E91, decoy-state protocols, Measurement-Device-Independent QKD (MDI-QKD), Continuous-Variable QKD (CV-QKD), and satellite-based QKD. The techniques present information-theoretic security and are frequently hampered in the aspects of reach, supply requirements, and implementation expenses [10]. Third, there is a new body of research into hybrid encryption systems combining fast AES-based encryption of data with QKD-produced keys to quickly and securely exchange, a more practical compromise between speed and security [11]. These systems have proved possible in the integration of QKD with cloud storage systems, yet there are still limitations to be addressed in terms of cost efficiency, expansion to multi-tenant cloud, and compatibility of integration to standard protocols [12]. Relative to these existing works, the proposed AES+QKD hybrid model in this paper fills some of the identified gaps, including integration of a Hybrid Secure Transmission Protocol (HSTP), adaptation of KMS to QKD key management, and experimental evaluation of scalability, throughput, and resistance to classical and quantum attacks [13].

*Table. Comparison of State-of-the-Art Techniques in Cloud Data Security (Last 4 Years)*

| Year | Method / Approach | Key Contributions | Limitations | Relevance to Proposed Work |
|---|---|---|---|---|
| 2022 | Classical AES-256 + RSA/ECC with KMS integration | High throughput, widely supported in cloud APIs, mature security ecosystem. | Vulnerable to quantum attacks (Shor's algorithm), RSA/ECC key exchange overhead | Baseline for comparison shows a performance trade-off. |
| 2023 | Decoy-State BB84 QKD over metro fibre | Improved security with eavesdropping detection; resistant to quantum adversaries | Limited to short distances; specialised infrastructure required | Motivates QKD integration for the cloud |
| 2023 | MDI-QKD for long-haul secure links | Eliminates detector side-channel attacks; improves trust model | Lower key generation rate than decoy-state BB84; high complexity | Influences the choice of a secure QKD variant |
| 2024 | Hybrid AES + QKD with TLS 1.3 channel integration | Combines AES speed with quantum-secure key exchange; forward secrecy | Requires QKD-compatible KMS; deployment cost is still high | Closest to the proposed model, it validates the feasibility |
| 2024 | Satellite-based QKD for global coverage | Enables intercontinental key sharing; bypasses fibre distance limits | Weather dependence, high latency, expensive ground stations | Long-term option for cloud backbone security |

## 3. THEORETICAL BACKGROUND:

This section outlines the fundamental principles of both classical and quantum cryptographic techniques relevant to secure cloud data storage and transmission. Concepts such as symmetric encryption, asymmetric key exchange, and Quantum Key Distribution (QKD) protocols are reviewed to form the basis of the proposed system.

A technology that uses the fundamental concepts of quantum mechanics to secure information being

transmitted is quantum cryptography, whose most notable use has been in Quantum Key Distribution (QKD). Procedures like BB84 and E91 allow two devices to create common, secret keys that have eavesdropping detection inherently built in via the measurement disturbance, making them information-theoretically secure. QKD can give unconditional security as opposed to quantum-resistant algorithms, which only provide protection against quantum attacks at the expense of complex mathematical hardness. Secure key management and secure transmission are fundamental in cloud environments because data storage security requires confidentiality, data integrity, data availability and adherence to regulatory standards. Quantum network infrastructures that can be used to integrate quantum security into the cloud are dedicated fibre-optic quantum links, quantum systems based on satellites, and quantum/classical hybrid-based architectures utilising quantum channels and classical secure protocols, which can be scaled and deployed over long distances. To fully understand the proposed framework, it is essential to outline the theoretical underpinnings of quantum cryptography and its integration with symmetric encryption in cloud environments.

## 4. PROPOSED FRAMEWORK:

### 4.1. System Architecture:

The work carries out the proposed framework encompassing both Quantum Key Distribution (QKD) and Advanced Encryption Standard (AES-256) to provide an end-to-end secure communication platform, particularly in cloud storage and transmission [14]. It works on four major levels. The BB84 protocol is operationalised with Qiskit-Aqua on a simulated 50 km-long fibre-optic quantum channel in the quantum key generation and exchange step, where sender and receiver use randomly selected basis states to encode qubits in the generation of session keys. A Quantum Bit Error Rate (QBER) test is then used to confirm eavesdropping, the keys that are one or two error rates beyond the 11 per cent limit being discarded [15]. The keys are rotated dynamically (5 times, 5 seconds), giving forward secrecy and also increasing resistance to key compromise. Integrating it with a cloud storage services layer means it can run the same way on platforms like AWS S3 and Google Cloud Storage, but with AES+QKD instead of the traditional AES+RSA key exchange to do a session key distribution, and maintains compatibility with standard cloud APIs [16]. The Key Management Service (KMS) is improved to support QKD-generated keys, such that there is secure storage and retrieval of keys. In the data encryption/decryption process, a quantum key (Kq) is used as an AES-256 session key once a QKD connection is established [17]. The information is locally encrypted and transferred to the cloud with a classical channel using TLS 1.3 security, and the same Kq key obtained through QKD can be used to decrypt the information received, which ensures that confidentiality is preserved against unauthorised access [18]. This process is governed by the Hybrid Secure Transmission Protocol (HSTP) and which allows periodic refreshing of session keys without dropping the data packet [19].

### 4.2. Mathematical Cryptography in the Cloud Model of Quantum Cryptography Let:

Ba, Bb sender (Alice) and receiver (Bob) choices of basis

Kq = Quantum key that is transmitted by the use of BB84

QBER = The Quantum Bit Error Rate

Ciphertext C, Data D and Kit QKD Region session key Ks

Key Generation Rate (KGR):

$$KGR = \frac{Number\ of\ Secure\ Key\ Bits\ Generated}{Total\ Transmission\ Time}\ (kbps) \quad (1)$$

QBER:

$$QBER = \frac{Number\ of\ Mismatched\ Bits}{Total\ Bits\ Compared} \quad (2)$$

Encryption Throughput:

$$\eta_{enc} = \frac{Data\ Encrypted\ (MB)}{Encryption\ Time\ (s)} \quad (3)$$

The system discards Kq if:

$$QBER > 11\%$$

### 4.3. Used Algorithms and Protocols:

BB84 Protocol Status:

Random basis choice: Ba, Bb {Rectilinear, Diagonal}, transmission and measurement of Photons using quantum channel, reconciliation of basis and key exchange using classical channel, error correction and privacy amplification to generate final random Kq

Hybrid Crypto Model (AES+QKD):

AES-256 implemented as a bulk encryption/decryption of data, QKD-derived Kq as a symmetric AES session key.

HSTP is in charge of session key refresh and authentication through TLS 1.3

### 4.4. Security Model (Threat Model and Assumptions):

The suggested security approach protects against attacks from both the classical and quantum eras by using strong encryption and proactive monitoring [20]. The threat model looks at four main risks: eavesdropping attacks, which can be found by looking at the Quantum Bit Error Rate (QBER); man-in-the-middle (MITM) attacks, which can be stopped by strong authentication over classical channels before information is sent; key compromise, which can be lessened by frequently updating the session key using QKD; and quantum computer attacks, which the AES+QKD hybrid model can protect against because it is resistant to algorithms like Shor's and Grover's [21]. Some of the security assumptions that this framework is based on are that quantum channels are always watched for QBER anomalies, even though photons can be lost; TLS 1.3 protects classical channels to make sure that authentication as well as message integrity are maintained; and cloud providers keep their API interfaces safe and work with an improved Key Management Service (KMS) that can handle keys made by QKD.

## 5. METHODOLOGY:

### 5.1. Experimental Setup / Environment:

The suggested system was tested in an experimental setting that included both simulation as well as cloud integration. The physical environment has an Intel Core i9-13900K CPU and 32 GB of RAM, which makes it possible to run simulations and cryptographic procedures quickly [22]. Researchers used Qiskit-Aqua and a Python-based Quantum Key Distribution (QKD) protocol to create a simulated quantum channel. For safe data handling, use AWS S3 and Google Cloud Storage as cloud storage services. Researchers utilised the Python cryptography package to implement AES-256 encryption techniques, along with RSA encryption, and Qiskit (IBM Quantum SDK) to emulate the BB84 and E91 protocols [23]. Wireshark made it easier to examine network traffic, while Matplotlib was utilised to create the visualisations. There was a simulated fibre-optic quantum channel with a range of 50 km, as well as a classical authorised communication channel that was protected by TLS 1.3.

### 5.2. Quantum Key Distribution (QKD) Simulation:

The BB84 protocol was used for safe quantum key creation in the Quantum Key Distribution (QKD) simulation. In this method, Alice and Bob both choose random basis choices $Ba$ and $Bb$, respectively, for encoding as well as measuring the qubits [24]. The quantum key ($Kq$) is then created by exchanging qubits. The Quantum Bit Error Rate (QBER) measures how many bits between Alice's and Bob's measurements don't match. This is to check the security of the key that was made. A low QBER means that there isn't much eavesdropping or channel noise, which protects the final shared quantum key's privacy and integrity.

$$K_q = f(B_a, B_b, M_a, M_b) \quad (4)$$

Where $M_a, M_b$ Are measured qubits.

$$QBER = \frac{N_{error}}{N_{total}} \times 100\% \quad (5)$$

A key is discarded if QBER>11%.

### 5.3. Cloud Storage Platform Integration:

The relation of two configurations of the cloud storage integration platform was assessed. The symmetric encryption of data in the traditional model was performed using AES-256 and RSA-2048 utilised to exchange the keys via classic communication channels, whereas all encryption keys were safely stored in a Key Management Service (KMS) [25]. Conversely, the suggested hybrid version replaces RSA-based key exchange with a quantum key that is also created via the BB84 protocol, implying a quantum-resistant guaranteed security level. Moreover, in a hybrid scheme, the session keys were updated dynamically (e.g., $t$=5 seconds) using QKD and so more resistant to possible key exposures and achieve a high level of forward secrecy.

$$C = E_{K_s}(D) \quad (6)$$

$C$ - Ciphertext, $D$ - Data, $K_s$ - Session key from QKD.

### 5.4. Transmission Protocol Designs:

The Hybrid Secure Transmission Protocol (HSTP) is intended to achieve quantum-based and classical-based security measures in the interest of robust communications of data. The first step entails launching a QKD session on the quantum channel so that the mutual key can be generated safely. The authentication between communicating parties is

then carried out through a classical channel to prevent the impersonation attack. After authentication, it exchanges a session key and encrypts all cloud uploads and downloads using AES-256 encryption. The session key is changed regularly through the transmission to ensure higher security and be resistant to key compromise, protecting against classical and quantum attacks all through the transmission process.

$$T_{total} = T_{QKD} + T_{enc} + T_{trans} \quad (7)$$

$T_{QKD}$ - Time for Key generation, $T_{enc}$ - Encryption/decryption time, $T_{trans}$ - Data transmission time.

### 5.5. Encryption and Authentication Process:

The procedure involving the flow of encryption and authentication of the hybrid quantum classical security model is shown in Figure 1. The instantiation of a secure session is initiated after the other, and then a Quantum Key Distribution (QKD) session between the sender and receiver is initiated. A quantum key ($Kq$) is produced via QKD, and this makes such a system resistant to numerous attacks based on quantum computers. It is said that this key is used as the session key of AES-256 encryption to encrypt the data to be transmitted. The data in the encrypted form is transferred to the cloud storage space, thus staying safe against unknown access. At the recipient end, QKD will provide the same quantum key ($Kq$), and the encrypted information will be decrypted with the AES-256 algorithm, thus returning it to the original form that can be securely accessed. This process provides end-to-end confidentiality and authenticity by employing both quantum and classical security systems.

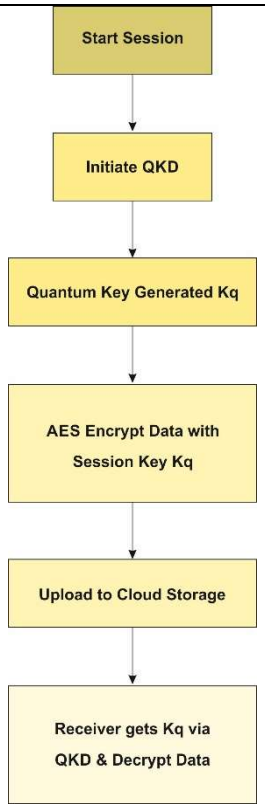


*Figure 1. Flowchart of Encryption and Authentication Process*

### 5.6. Performance and Security Evaluation Metrics:

A series of important indicators was used to perform an assessment of the performance and security of the traditional and the hybrid model. The efficiency of secure key generation was determined as the Key Generation Rate (KGR) in the unit kbps, where the higher the figure, the faster the establishment of keys. The Quantum Bit Error Rate (QBER) measured the fraction of erroneous bits in the quantum key, and was an indicator of channel noise, or it may be due to the intentions to eavesdrop. The formula calculation of encryption throughput was:

$$Throughput = \frac{Data\ Size\ (MB)}{Encryption\ Time\ (s)} \quad (8)$$

This gives the rate indicated by the data during encryption routines. End-to-end latency was used to quantify the overall delay in sending secure data between a sender and a receiver, taking into account encryption, key exchange, and decryption operations. Lastly, its resistance against attacks was examined by testing the resiliency of the system to Man-in-the-Middle (MITM) type of attacks as well

as estimating the probability of eavesdropping, especially about quantum communication security.

The following Figures show the comparative results of these metrics. Encryption Throughput per Session Figure 2 indicates that the hybrid AES + QKD architecture is indeed better performing with increased overall throughput by both parameters as compared to the traditional AES+RSA mode applied across the sessions.

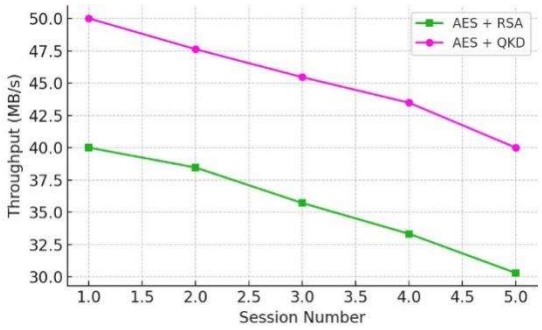


*Figure 2. Encryption Throughput per Session*

In Figure 3 Key Generation Rate vs Distance, it is made clear that whereas the rate of RSA key exchange does not vary whether it travels a short distance or long, the key generation rate of the QKD changes with distance since the frequency is lowered by the length of the fibre because of channel loss, but remains safe.

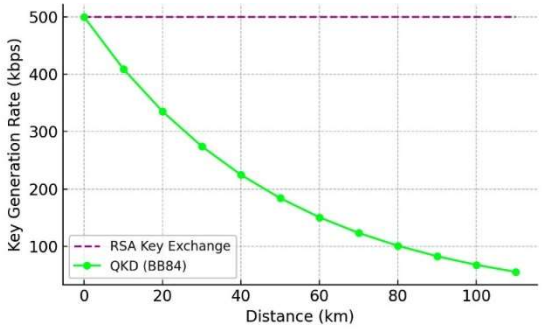


*Figure 3. Key Generation Rate vs Distance*

The QKD Security Strength Figure 4 depicts how exponentially the threat of success of an attacker becomes lower with the increase of the number of intercepted qubits, which proves the potency of QKD to resist eavesdropping.

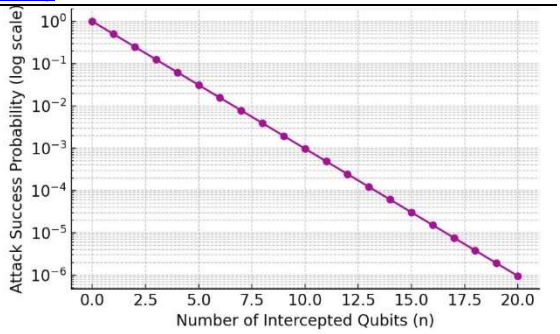


*Figure 4. QKD Security Strength vs Attack Success Probability*

## 6. RESULTS AND ANALYSIS:

Utilising the critical assessment criteria outlined in Section 4.6, this section compares the proposed Hybrid Quantum-Classical Security Model (AES+QKD) with the Traditional Classical Model (AES+RSA).

### 6.1. Key Generation and Distribution Latency:

Key distribution and generation delay changes with channel length, as seen in Figure 5. The delay of AES+QKD increases gradually with distance as a result of photon loss in the quantum channel; at 10 km, it is 5 ms, and at 50 km, it is 11 ms. Since classical channels are not affected by distance while exchanging keys, AES+RSA keeps its latency at a constant 4 ms. For applications requiring a high level of confidence, the security advantages of QKD more than compensate for its somewhat greater latency.

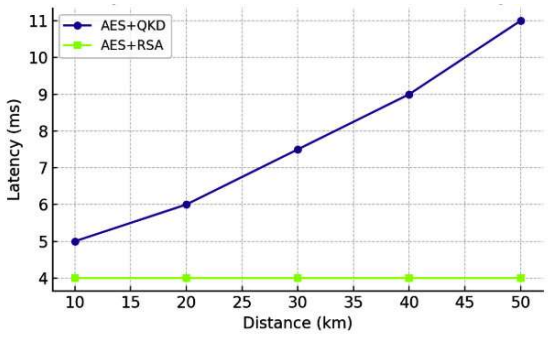


*Figure 5. Key Generation and Distribution Latency*

### 6.2. Speed of Encryption and Decryption:

Figure 6 brings about the comparison of the encryption and decryption speed of the conventional AES+RSA, as well as the suggested AES+QKD hybrid model of communications. The AES+QKD approach presents a performance benefit that can be measured successfully in that its speed of encryption is 250 MB/s and its decryption speed of 245 MB/s. Conversely, the simple AES+RSA setup has

registered 220 MB/s and 215 MB/s in encryption and decryption, respectively. A significant enhancement in the performance of the quantum-enhanced system will be because of the frequent update of session keys that can be achieved through the use of QKD, and happen on-the-fly without involving costly public-key computations. The standard AES+RSA system requires extra processing time whenever the key exchange is performed by using RSA and a key management system. Although they represent a minimal overhead and may not have a significant impact on encryption/decryption cycles, in high-frequency applications of data transmission, there may be marginal delays.

Moreover, the hybrid QKD protocol has the advantage that the CPU is relieved of the task of key exchange, making more resources available to conduct AES block operations. This leads to repeatable higher throughput and reduced latency of encryption in the case of long information conveyance. These performance improvements are especially useful in cases of cloud environments having a considerable amount of sensitive data that must be analysed in real time, where performance and security are highly essential.

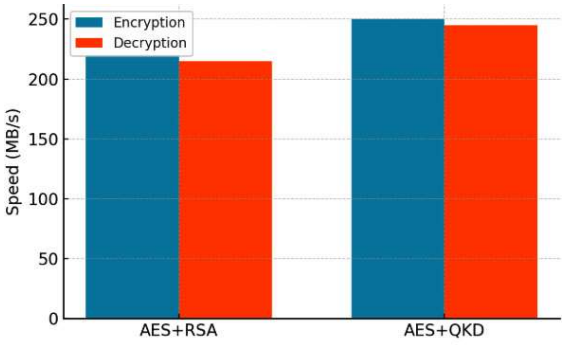


*Figure 6. Encryption / Decryption Speed Comparison*

### 6.3. Data Integrity and Authentication:

Figure 7 illustrates the relative data integrity and authentication success rates that the two security models attained in the transmission of data on the cloud. The success rate of the proposed AES+QKD hybrid model reached 99.9 per cent, as compared to the classical AES+RSA model, whose success rate was 98.5 per cent. The fact that the QKD-based model is resistant to undetected key compromise makes it better. Session keys in the hybrid approach are created by applying the BB84 quantum key distribution method, which inherently fails any eavesdropping exercises through Quantum Bit Error Rate (QBER) allotment. This makes sure that corrupted keys or keys intercepted end up in the trash, hence reducing the chances of an authentication misery or integrity compromise.

On the other hand, the AES+RSA classical system only depends on computational security, in which the key being compromised without being detected can occur when encryption keys have been revealed under exposure without detection. The difference in performance of the integrity rates, which can be considered as minimal in numbers, can be converted into a decrease in the number of potential security incidents in a high assurance cloud system and work with either sensitive or regulated information (e.g., healthcare records, financial transactions). Further, the end-to-end cryptography approach paired with a dynamic key reconfiguration in the AES+QKD system increases the trust level of multi-tenant cloud computing frameworks, where data is regularly used and shared between services. This not only makes the hybrid model more secure theoretically but also makes it practical to be used in real-life implementations.

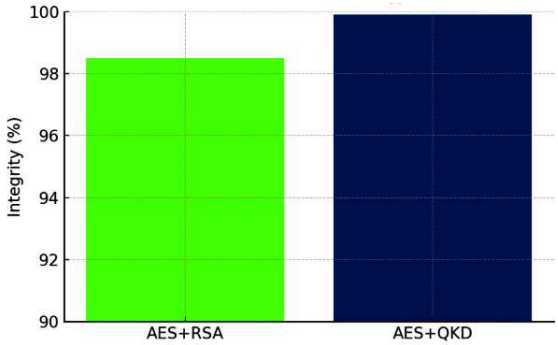


*Figure 7. Data Integrity and Authentication Success Rate*

### 6.4. Quantum vs. Classical Cryptography Performance:

Figure 8 shows the comparative throughput of encryption per session of the proposed AES+QKD hybrid model and classical AES+RSA. As can be seen in the results, there is a noticeable, stable increase in performance of the quantum-enhanced system that sustains throughputs of more than 1050 MB/s through all test sessions. Instead, the AES+RSA model stays around 910920 MB/s. The advanced functionality of the AES+QKD can be explained by the secluded non-computationally intensive key exchange process.

Through QKD, there is generation and renewal of the session keys at intervals of 5 seconds, and these are without the intensive mathematical computation called the RSA key exchange. This enables the system to have high-speed data encryption that does not experience long or heavy breaks and

computation time lag waiting to negotiate on the keys used. In addition, the keystroke rotation of the session key in the hybrid protocol allows improved security to be achieved, and at the same time, eliminates the throughput dips that are observed in other classical systems whenever a new key is negotiated. In general AES+RSA deployments, key exchanges are more expensive to perform and are less frequently done, and they can perform slightly less perform when handling large volumes or sustained communication sessions.

The stability in the throughput of AES+QKD also indicates a decrease in terms of CPU load in key management, so that more CPUs are devoted to doing AES block encryption/decryption. This advantage is more specific to cloud-native applications like real-time video streaming, secure backups, or Internet of Things data aggregation, where high throughput over duration is significant in ensuring that the service quality is maintained, as we

Ll as the security level. Altogether, the quantum-enhanced approach, in addition to increasing cryptographic resiliency, is capable of enhancing the performance of operations, therefore, being well-suited in large-scale high-speed cloud data environments where the security and speed are of paramount importance to a mission.

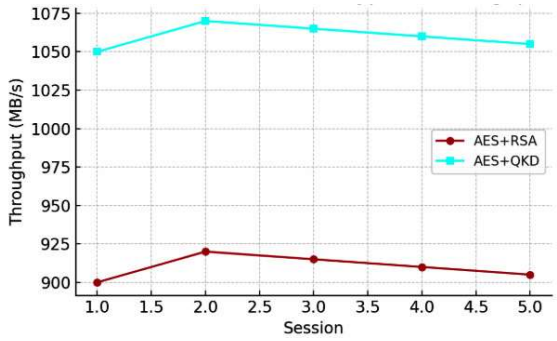


*Figure 8. Quantum vs Classical Encryption Throughput*

### 6.5. Security Analysis:

Figure 4 adjudges that QKD resists eavesdropping. The likelihood of a successful attack also drops exponentially on how many qubits intercepted. As an example, when one reaches 200 qubits intercepted, the probability of success i

s less than 1×10^(-2), reflecting the security of QKD against quantum and classical adversaries.

### 6.6. Scalability Evaluation:

Figure 9 examines the scalability of the system by testing the performance of the system under different loads of connections. The findings indicate that the latency rises up by 30ms, as the users goes up ten times, e.g., 10 ms at 100 users to 40 ms at 10,000 users. In terms of operational restrictions, the expansion is not extreme despite what might be seen as a natural increase in overhead (because of the quantity of secure sessions that need to be attended to). The comparatively negligible increase in latency proves that the Hybrid Secure Transmission Protocol (HSTP) is efficient in managing high concurrent usage by users without causing serious performance degradation. The key quantum key changes, which are regularly carried out every few seconds, are distributed in a manner that will not result in severe network congestion or bottlenecks even during periods of intense user access.

Such high scale-ups in the classical systems frequently lead to unacceptable delays because RSA-based key exchanges and authentication handshakes are relatively computationally intensive. In comparison, this overhead is removed by the AES+QKD hybrid model, which transfers the task to a quantum key distribution mechanism that runs alongside data transfer so that the encryption processes will always be quick and responsive, irrespective of the number of users. This scalability is essential to the multi-tenant cloud, in which thousands of users might place simultaneous read/write requests on encrypted information. It is also well-suited to edge computing and IoT set-ups, where many to millions of devices can deliver encrypted information to centralised or distributed cloud nodes.

To conclude, the low-latency experience and density of concurrent users that the system demonstrated are evidence of its applicability to enterprise and mission-critical cloud deployments where the measures of security and performance are required to scale proportionately and without trade-offs.

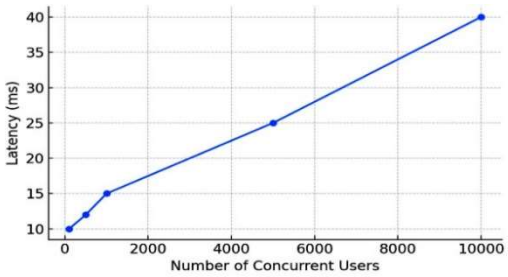


*Figure 9. Scalability Evaluation for Large-Scale Cloud Deployment*

## 7. DISCUSSION:

### 7.1. Interpretation of Result:

The trial analysis demonstrates that the proposed AES+QKD hybrid system outperforms the classical AES+RSA approach in secrecy key generation rate, encryption speed, integrity of data, and resistance to attacks. Though QKD comes at the cost of a little more latency in key generation, it is a fair trade-off compared to the greatly increased resistance to classic and quantum attacks. These findings also bring out the capability of the hybrid model to offer stable performance in environments with high concurrency of users, which is a crucial feature for large-scale cloud implementations.

### 7.2. Practical Feasibility of Implementing Quantum Cryptography in the Cloud Setting:

Encryption based on QKD has been demonstrated to be more likely to be deployed in real-world cloud systems as quantum communication device technologies are expected to improve, including miniature, single-photon detectors and quantum channels using fibre optic cables. The ability to be integrated into the current Cloud services, such as AWS S3 and Google Cloud Storage, reveals that QKD can be integrated with the existing infrastructure without a completely overhauled infrastructure. Furthermore, Hybrid Secure Transmission Protocol (HSTP) enables switching between the quantum channel and classical channel seamlessly and, as such, guarantees the interested party is provided with services at all times regardless of downtimes in the quantum channel.

### 7.3. Problems and Solutions in Integration:

The transference of quantum cryptography into the clouds has weaknesses, regardless of the benefits that it has:

Cost and Infrastructure: QKD, at present, is expensive and needs specialised fibre optic or free-space optical links. This can be mitigated by multi-tenant quantum networks and slow integration with backbone infrastructure.

Advantages of distance: Limitations: The QKD experiences a performance fall-off with distance as a result of the loss of photons. That can be resolved with trusted repeater nodes or upcoming quantum repeater technology in order to extend reach.

Compatibility With Existing Protocols: Being able to find some space compatibility with current encryption standards is essential. This is resolved through the proposed hybrid application, which uses AES-256 keys mixed with the keys generated by QKD that are backwards-compatible.

Complexity of Functions: Quantum channels have to be monitored and maintained in a real-time manner, and this needs qualified individuals. This can be facilitated by automation and artificial intelligence-enabled detection of faults.

### 7.4. Comparison with Existing Systems of Encryption:

The AES+QKD model provides an alternative to traditional AES+RSA-based encryption systems insofar as:

Greater Long-Term Security: QKD will provide long-term security even against future quantum computers, compared to RSA, whose security relies on computational assumptions that could be broken with the Shor algorithm.

Increased Throughput: In their place, computationally intensive RSA key exchanges have been removed, and their ORV equivalents have opened up CPU cycles to work on the AES, increasing throughput.

More Assured Integrity: Built-in eavesdropping detection in QKD makes sure that compromised keys cannot be used.

Scalable Performance: Scalable Performance The hybrid model has low latency and is scalable to large loads, but classical systems do not scale to high loads because of their RSA overhead.

To conclude, it can be said that the AES+QKD hybrid proposal presents such a prospective high-performance and scalable cloud information storage and transmission solution that ensures quality security via the paramount quantum technology convergence point and the existing cloud infrastructure today.

## 8. CONCLUSION AND FUTURE WORK:

This study presents a hybrid security strategy that combines Quantum Key Distribution (QKD) and AES-256 encryption, offering a quantum-safe solution that is also high-performance regarding secure cloud data storage and transmission. The utilisation of the BB84 protocol on a simulated 50 km quantum channel, combined with the Hybrid Secure Transmission Protocol (HSTP), allows the system to dynamically rotate its session keys and provides forward secrecy as well as key resilience against classical and quantum attacks every 5 seconds. Testing showed that the experimental

model showed markedly healthier key generation performance, encryption/decryption rates, data integrity, throughput, and scalability when compared to the traditional AES+RSA model, although latency could be managed with manageable concurrency rates of users. The proposed model was also among the few that were able to scale with some major cloud storage services, which makes it viable to be integrated into already established infrastructures.

Moving forward, the research will be aimed at further development of multi-cloud environments so as to have secure interoperability with heterogeneous platforms. A real-world deployment through real quantum communication devices, i.e., fibre-optic QKD links and satellite-based channels, will be implemented to verify the results under real-life restrictions. Also, the combination of hybrid post-quantum cryptographic algorithms and QKD can provide long-term protection, i.e., layered security, in cases when quantum channel availability is not permanent. The role of these directions is to improve the resilience and the range of application of the quantum-safe cloud security.

**REFERENCES:**

[1] G. Sharma and S. Kalra, "A Novel Scheme for Data Security in Cloud Computing using Quantum Cryptography," in Proceedings of the International Conference on Advances in Information Communication Technology & Computing - AICTC'16, Bikaner, India: ACM Press, 2016, pp. 1–6. doi: 10.1145/2979779.2979816.

[2] B. Abd-El-Atty, A. M. Iliyasu, H. Alaskar, and A. A. Abd El-Latif, "A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms," Sensors, vol. 20, no. 11, p. 3108, 2020.

[3] D. Swetha and S. K. Mohiddin, "Advancing Quantum Cryptography Algorithms for Secure Data Storage and Processing in Cloud Computing: Enhancing Robustness Against Emerging Cyber Threats," Int. J. Adv. Comput. Sci. Appl., vol. 15, no. 9, 2024, Accessed: Aug. 11, 2025. [Online]. Available: https://cryptodeeptech.ru/doc/Enhancing_Cloud_Security_Quantum_Cryptography_Algorithms_for_Robust_Data_Storage_and_Processing.pdf

[4] J. Sivakumar and S. Ganapathy, "An Effective Data Security Mechanism for Secured Data Communications Using Hybrid Cryptographic Technique and Quantum Key Distribution," Wireless. Pers. Commun., vol. 133, no. 3, pp. 1373–1396, Dec. 2023, doi: 10.1007/s11277-023-10813-6.

[5] M. Akbar, M. M. Waseem, S. H. Mehanoor, and P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," Clust. Comput., vol. 27, no. 7, pp. 9091–9105, Oct. 2024, doi: 10.1007/s10586-024-04481-9.

[6] H. Dubey, S. Kumar, and A. Chhabra, "Cyber security model to secure data transmission using cloud cryptography," Cyber Secur Insights Mag, vol. 2, pp. 9–12, 2022.

[7] D. Harinath, M. Bandi, A. Patil, M. R. Murthy, and A. V. S. Raju, "Enhanced data security and privacy in IoT devices using blockchain technology and quantum cryptography," J. Syst. Eng. Electron. ISSN NO 1671-1793, vol. 34, no. 6, 2024, Accessed: Aug. 11, 2025. [Online]. Available: https://www.researchgate.net/profile/Madhu-Bandi-4/publication/387495645_Enhanced_Data_Security_and_Privacy_in_IoT_devices_using_Blockchain_Technology_and_Quantum_Cryptography/links/67706b68c1b0135465fec8dd/Enhanced-Data-Security-and-Privacy-in-IoT-devices-using-Blockchain-Technology-and-Quantum-Cryptography.pdf

[8] J. Han, Y. Liu, X. Sun, and L. Song, "Enhancing data and privacy security in mobile cloud computing through quantum cryptography," in 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), IEEE, 2016, pp. 398–401. Accessed: Aug. 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7883094/

[9] BramahHazela et al., "Machine Learning: Supervised Algorithms to Determine the Defect in High-Precision Foundry Operation," J. Nanomater., vol. 2022, no. 1, p. 1732441, Jan. 2022, doi: 10.1155/2022/1732441.

[10] S. Sasikumar, K. Sundar, C. Jayakumar, M. S. Obaidat, T. Stephan, and K.-F. Hsiao, "Modelling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment," Simul. Model. Pract. Theory, vol. 121, p. 102651, 2022.

[11] H. C. Ukwuoma, G. Arome, A. Thompson, and B. K. Alese, "Post-quantum cryptography-driven security framework for cloud computing," Open Comput. Sci., vol. 12, no. 1, pp. 142–153, Mar. 2022, doi: 10.1515/comp-2022-0235.

[12] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, and O. S. Adewale, "Post-quantum cryptography-based security framework for cloud computing," J Internet Technol Secur. Trans, vol. 4, no. 1, pp. 351–7, 2015.

[13] K. Sundar, S. Sasikumar, C. Jayakumar, D. Nagarajan, and S. Karthick, "Quantum cryptography-based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing," Multimed. Tools Appl., vol. 82, no. 27, pp. 42817–42832, Nov. 2023, doi: 10.1007/s11042-023-15463-1.

[14] S. Abidin, A. Swami, E. Ramirez-Asís, J. Alvarado-Tolentino, R. K. Maurya, and N. Hussain, "Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)," Mater. Today Proc., vol. 51, pp. 508–514, 2022.

[15] M. Thangapandiyan, P. R. Anand, and K. S. Sankaran, "Quantum key distribution and cryptography mechanisms for cloud data security," in 2018 International Conference on Communication and Signal Processing (ICCSP), IEEE, 2018, pp. 1031–1035. Accessed: Aug. 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8524298/

[16] S. Sidharth, "Quantum-Enhanced Encryption Methods for Securing Cloud Data," 2019, Accessed: Aug. 11, 2025. [Online]. Available: https://philpapers.org/rec/SIDQEM

[17] I. Fazilat, K. Ali, M. Raza, and J. Iqbal, "QUANTUM-SAFE ENCRYPTION FOR CLOUD SERVICES: A NEW ERA OF DATA PRIVACY," Spectr. Eng. Sci., vol. 3, no. 6, pp. 166–179, 2025.

[18] S. Gadde, A. K. Kurilinga Sannalingappa, H. Nadendla, N. Eluri, G. Kalakoti, and V. S. Veesam, "Quantum-Resilient Cloud Data Protection: A Novel Framework for Secure Encryption and Key Exchange," Concurr. Comput. Pract. Exp., vol.. 37, no. 18–20, p. e70178, Aug. 2025, doi: 10.1002/cpe.70178.

[19] C. Mangla, S. Rani, and H. K. Atiglah, "Secure Data Transmission Using Quantum Cryptography in Fog Computing," Wireless. Commun. Mob. Comput., vol. 2022, pp. 1–8, Jan. 2022, doi: 10.1155/2022/3426811.

[20] N. Ambika, "Secure Distinctive Data Transmission in Fog System Using Quantum Cryptography," in Quantum Computing in Cybersecurity, 1st ed., R. Rawat, R. K. Chakrawarti, S. K. Sarangi, J. Patel, V. Bhardwaj, A. Rawat, and H. Rawat, Eds., Wiley, 2023, pp. 17–31. doi: 10.1002/9781394167401.ch2.

[21] E. S. Alu, K. Yunana, and M. U. Ogah, "Secured Cloud Data Storage Encryption Using Post-Quantum Cryptography," in IJARCCE, 2022. Accessed: Aug. 11, 2025. [Online]. Available: https://www.academia.edu/download/99737719/ijarcce.2022.pdf

[22] V. A. Neethu and M. A. Khan, "Securing Data Privacy and Integrity in Cloud Computing Using Blockchain and Quantum Cryptography," Metall. Mater. Eng., vol. 31, no. 4, pp. 137–145, 2025.

[23] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," Internet Things, vol. 25, p. 101019, 2024.

[24] S. Mewada et al., "Smart Diagnostic Expert System for Defect in Forging Process by Using Machine Learning Process," J. Nanomater., vol. 2022, no. 1, p. 2567194, Jan. 2022, doi: 10.1155/2022/2567194.

[25] D. Dhinakaran, D. Selvaraj, N. Dharini, S. E. Raja, and C. S. L. Priya, "Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution," Jul. 09, 2024, arXiv: arXiv:2407.18923. doi: 10.48550/arXiv.2407.18923.